Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 12 | Dec 2017

# SECURE OF WEB-ACCOUNTS USING PERSONAL-PCFG

Vaishnavi Mahajan [1] | Pratima Nikam [1] | Kalyani Padmawar [1] | Nihar Ranjan [1]

[1] Computer Department, Sinhgad Institute of Technology & Science, Pune, India - 411041.

## ABSTRACT

For security of the data as well as maintaining privacy over the internet, authentication is used. For this the password is used but the user uses small password, easy to memorize password or password which can be guessed easily. People use personal information as their password for easy memorization. In this paper, we analysis the various passwords from the leaked dataset to research their personal information for finding the relation between them and the password. We use Probabilistic Context-Free Grammars (PCFG) method with semantic-rich method to propose Personal-PCFG method. This method will help us to crack the password much faster than the PCFG method which increases the chances of successful password crack. To protect user from this type of attacks we use distortion function.

**KEYWORDS:** Cyber security, Information security, PCFG.

## 1. INTRODUCTION:

Network security sometime is calling the InfoSec i.e. information Security. Information security is the no of strategies for the extract the process. Tools. It's required the varies policies necessary to prevent, detect document and find the threats to digital and non-digital information. Information security is the responsible for a set of business processes that provide security to information assets. It secures all the business and personal information.

Information security threats come in large quantity in different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are the main objective is to help user to choose strong password which will be difficult for the hacker to crack password. User mostly use easy password for its memorization. Mostly this password contains personal information which makes it vulnerable. Hacker can get user information from various sources like Facebook. This information can be used by hacker for guessing password.

The prime focus of this is to help user to choose strong password. Mostly people use their information in passwords. Hackers can get the peoples information from various sources like Social Networking Site. This information can be used to guess user passwords. If the user's password does not contain personal information then it is difficult for the hacker to crack the password.

## 2. MATERIALS AND METHODS:

In this system user enters the personal information and enter the Username and Password. First the user system take password information and search into the user fill the information. Then it's finding the correlation of that password by using the PCFG algorithm. After that by using the simple Distortion function user enter password to Mix with dictionary of password and providing the strong password to the user.

**Proposed Algorithm :**

1) *Input:* All Personal Information and Password
2) *Output:* Strong Password
3) Collect all the information and password
4) Find Correlation between the information and password using Probability Context Free Grammar with sematic rich algorithm
5) If the password contains the user's personal information and weak password then the user has to create password. If the password is strong then password will be mixed with the complicate password from the dictionary.
6) The strong password will be mailed to the user.

## 3. RESULT:

To Secure User's Web Accounts from hackers and some attacks like bruteforce or dictionary attacks by providing strong password.

- It will protect users account from various attacks.
- It will increase password security.
- It will improve online authentication systems.

## 4. DISCUSSION:

The motivation of this paper is to increase the password security, as many researchers have proposed different authentication mechanisms, but no alternative can bring all the benefits of passwords without introducing extra burdens to users. Many times user used to give password which will be easily memorized or related to the user's personal information, but at the same time it would be benefit for the hacker who can easily hack the password by using the personal information of the user. Therefore to increase the security of the application we have proposed this paper which will be used to secure application by giving the strong password to the user. In this Strong password will be send to the valid users so that only valid user can authenticate the application by entering the strong password to the application. In this we assess the usage of names in other leaked password datasets that do not come with any personal information. To demonstrate the security vulnerability induced by using personal information in passwords, we propose a semantics-rich Probabilistic Context- Free Grammars (PCFG) method called Personal-PCFG, which extends PCFG by considering personal information symbols in password structures. We present simple distortion functions to defend against these semantics-aware attacks such as Personal-PCFG. Our evaluation results demonstrate that distortion functions can effectively protect passwords by significantly reducing the unwanted correlation between personal information and passwords.

## 5. CONCLUSION:

In this paper we are providing security to the application, to systematically analyze personal information in passwords. In many application users provide their personal information to the system while registration, Sometimes users to include their name in passwords, since it will be easier for the hacker to hack the password by using their personal detail. Therefore this paper introduced serious involvement of personal information in password creation, which makes a user password more vulnerable to a targeted password cracking. Therefore in this paper we develop Personal-PCFG based on PCFG which consider more semantic symbols for cracking a password. Personal-PCFG generates personalized password guesses by integrating personal information in the guesses. We also propose using distortion functions to protect weak passwords that include personal information. Our experimental results that Personal-PCFG is faster than PCFG in password cracking and eases the feasibility of mounting online attacks

**Acknowledgments:**

Our first and foremost acknowledgment is to our guide Mr. Nihar Ranjan. During the long journey of this study, he has supported us in every aspect. He was the one who helped and motivated us to propose research in this field and inspired us with his enthusiasm on research, his experience, and his lively character.

We express true sense of gratitude to my guide Mr. Nihar Ranjan for his perfect valuable guidance, all the time support and encouragement that he gave us.

We would like to thanks our head of department Prof. Mr. Nihar Ranjan, for inspiring us and providing all lab and other facilities.

*Name of the Student:* Vaishnavi Mahajan, Kalyani Padmawar and Pratima Nikam.

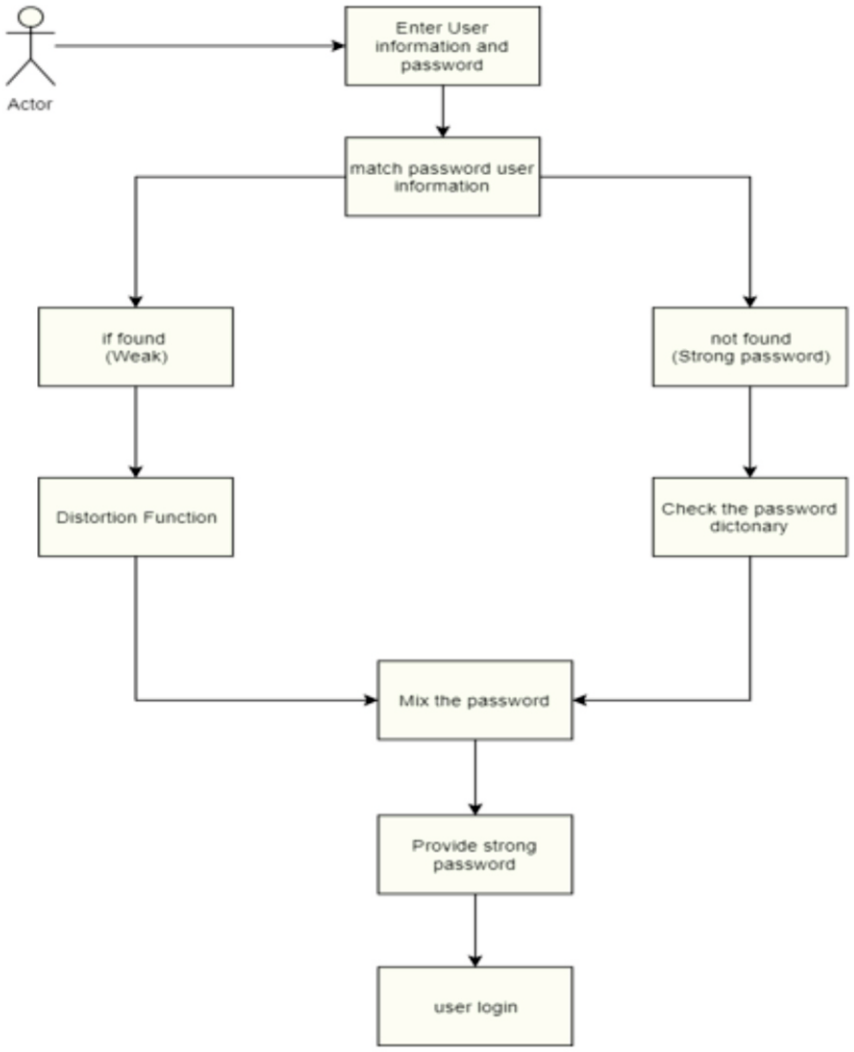


**Fig 1: Architecture Diagram**

**REFERENCES:**

1. J. H. Seo, K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption. In: Cryptographers" Track at the RSA Conference. Springer Berlin Heidelberg. 2013; 343-358.
2. J. Shao, Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption". Information Sciences, 2012; 206, 83-95.
3. J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System". IEEE Transactions
4. K. Liang, Z. Liu, X. Tan, D. S. Wong, C. Tang, "A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: International Conference on Information Security and Cryptology". Springer Berlin Heidelberg. 2012; 231-246.
5. L. Ferretti, M. Colajanni, M. Marchetti,"Distributed, concurrent, and independent access to encrypted cloud databases". IEEE transactions on parallel and distributed systems, 2014; 25(2), 437-446. on Computers, 2016; 65(6), 1992-2004.
6. J. H. Seo, K. Emura,"Efficient delegation of key generation and revocation functionalities in identity-based encryption. In: Cryptographers" Track at the RSA Conference. Springer Berlin Heidelberg. 2013; 343-358.
7. J. Shao, Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption". Information Sciences, 2012; 206, 83-95.
8. J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System". IEEE Transactions
9. K. Liang, Z. Liu, X. Tan, D. S. Wong, C. Tang, "A CCA-secure identity-based conditional proxy re-encryption without random oracles". In: International Conference on Information Security and Cryptology. Springer Berlin Heidelberg. 2012; 231-246.
10. L. Ferretti, M. Colajanni, M. Marchetti, "Distributed, concurrent, and independent access to encrypted cloud databases". IEEE transactions on parallel and distributed systems, 2014; 25(2), 437-446. on Computers, 2016; 65(6), 1992-2004.